Dispositivo de encriptado multirrol multimodo R&S®MMC3000

Seguridad reforzada en HF/VHF/UHF/SatCom para voz y datos

ROHDE&SCHWARZ

Comunicaciones Seguras

Folleto del Producto | 03.00

Dispositivo de encriptado multirrol multimodo R&S®MMC3000

Generalidades

El R&S®MMC3000 es un dispositivo táctico totalmente reforzado utilizado para cifrar y descifrar comunicaciones de voz y datos con el máximo nivel de seguridad. Con certificación TEMPEST, ofrece interoperabilidad para equipamiento de radio HF/VHF/UHF, comunicaciones vía satélite y de transmisión en línea. Es idóneo para la implementación en plataformas estacionarias y móviles bajo condiciones severas, así como en entornos navales y aéreos.

El R&S®MMC3000 ofrece los modos simplex, semi-dúplex y dúplex para satisfacer los requerimientos de la más extensa gama de aplicaciones digitales y analógicas, tanto para la operación local como remota. La operación del R&S®MMC3000 puede realizarse bien con una unidad de control o bien con el módulo de bus MIL. Un algoritmo de encriptado personalizable asegura la particularidad y exclusividad necesarias para los diferentes escenarios nacionales y de coalición.

En el modo de encriptado de datos, el dispositivo se integra perfectamente en sistemas de transmisión de datos equipados con interfaces militares estándar (están contempladas la mayoría de las interfaces militares estándar). El vocoder aplicado en el modo de voz optimiza la nitidez de la comunicación incluso en transmisiones con interferencias de ruido. El diseño flexible y orientado a futuras ampliaciones incluye un proceso de descarga de software protegido y una ranura para un módulo de encriptado adicional para la actualización del dispositivo de cara a futuras exigencias.

El R&S®MMC3000 incorpora una amplia gama de accesorios para su integración en infraestructuras de comunicación complejas. Además de un sistema de administración de seguridad (R&S®SMS3000), se añaden un dispositivo de carga de datos (DLD), clave de ignición de encriptado (CIK), armazón de montaje, fuente de alimentación y componentes para la operación remota de la unidad de control.

Datos clave

- Encriptado de voz y datos con los niveles de seguridad más elevados
- Protección de HF/VHF/UHF, SatCom y transmisión en línea
- Totalmente reforzado, protegido contra manipulaciones, certificación TEMPEST
- Implementación estacionaria y móvil en todos los ámbitos militares (ejército de tierra, marina, fuerzas aéreas)
- Algoritmos de encriptado personalizables para necesidades específicas del usuario

Dispositivo de encriptado multirrol multimodo R&S®MMC3000

Ventajas y características principales

Interfaces de operador dedicadas para diferentes aplicaciones

- Interfaz de administración de sistemas de software de control remoto
- Interfaz de administración de sistemas de comunicación por bus MIL
- Interfaz del usuario para la unidad de control
- Interfaz de auriculares/intercomunicación

▷ página 4

Protección integral gracias a un sofisticado concepto de seguridad

- Entorno de producción auditado
- Separación de hardware rojo-negro y protección contra manipulaciones
- Generación y gestión segura de claves

▷ página 6

Versatilidad a través de múltiples modos de tráfico/operación y métodos de transmisión

- Modos de tráfico adaptados a los modos de operación y métodos de transmisión
- Modos de operación para transmisiones de voz y de datos
- Teletipo para una fiabilidad extrema en las comunicaciones
- Preparado para transmisiones vía IP
- Transmisiones síncronas y asíncronas a través de las interfaces roja y negra

▷ página 8

Alta calidad de servicio y operación flexible con tecnología de vanguardia

- Alta calidad de servicio
- Configuración flexible
- Posibilidad de actualización

▷ página 10

Configuración individual mediante algoritmos de cifrado personalizables para requerimientos específicos del usuario

▷ página 11

Operación y puesta en servicio simplificada con una amplia gama de accesorios

- Un PC de configuración aumenta la eficiencia y precisión del proceso de carga de ajustes predefinidos
- La clave de ignición de cifrado (crypto ignition key, CIK) añade un nivel de seguridad adicional e incrementa la flexibilidad en la implementación
- El armazón de montaje protege al dispositivo en entornos con condiciones físicas severas
- El dispositivo de carga de datos R&S®GP3000 (DLD) facilita la distribución de claves a unidades distribuidas geográficamente
- Fuente de alimentación externa de adaptación continua (110 V/240 V)

▷ página 12

Interfaces de operador dedicadas para diferentes aplicaciones

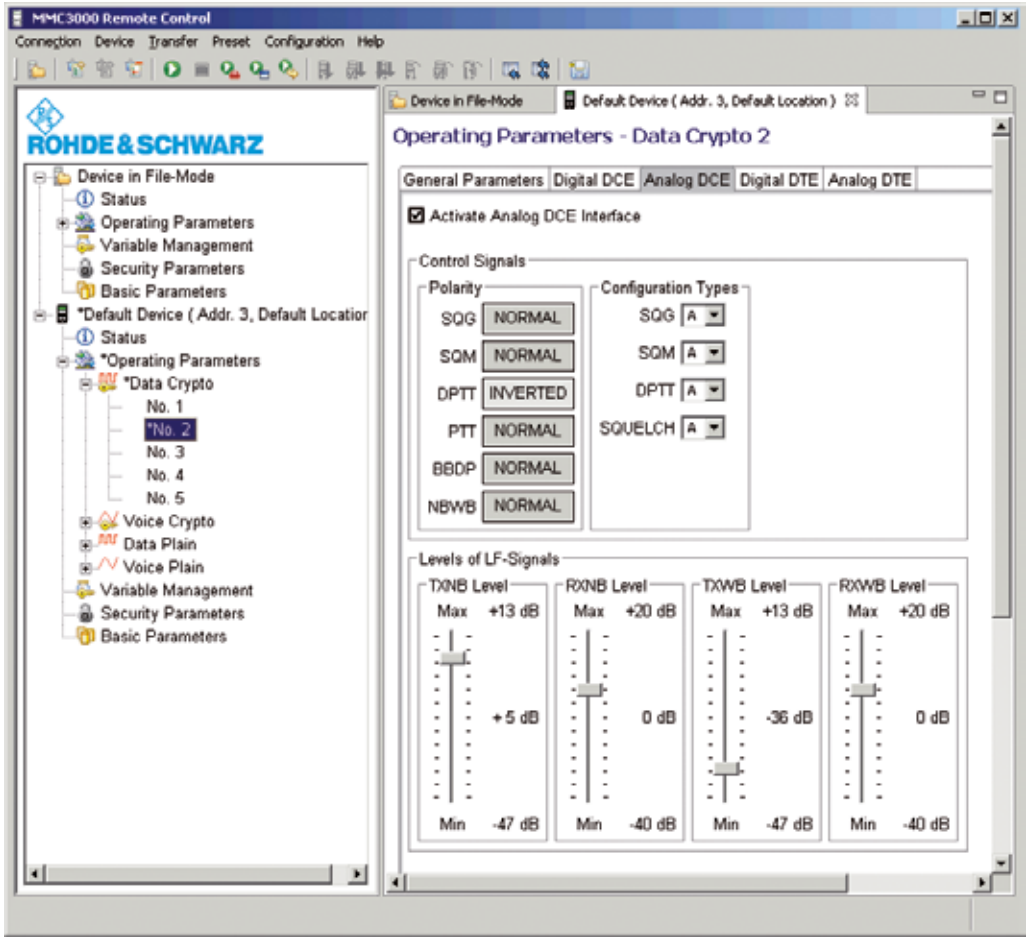
El R&S®MMC3000 ofrece un extenso repertorio de opciones de interfaz de operador para diferentes plataformas de aplicación y escenarios.

Interfaz de administración de sistemas de software de control remoto

El control remoto con plena funcionalidad en un entorno de software definido permite gestionar dispositivos en ubicaciones de difícil acceso, p. ej. habitáculos con poco espacio en aviones o en barcos. La aplicación aumenta la flexibilidad, precisión y velocidad a la hora de gestionar un sistema complejo, puesto que permite conectar hasta 31 R&S®MMC3000 al adaptador RS-485 a serie. Además, reduce la probabilidad de errores y ahorra recursos mediante la copia de ajustes repetitivos o la descarga de ajustes preparados. Se pueden almacenar ajustes predefinidos para una gran cantidad de dispositivos.

La aplicación también permite copiar y descargar parámetros predefinidos (p. ej. de un dispositivo a otro). Las cinco visualizaciones para cada dispositivo (estado, parámetros de operación, gestión variable, parámetros de seguridad y parámetros básicos), así como las actividades de supervisión, proporcionan una visión general completa y rápida de todos los dispositivos de un grupo o una vista de todos los ajustes de los dispositivos individuales en síntesis.

A través de la aplicación de control remoto, el operador puede cambiar fácilmente entre los ajustes predefinidos, adaptar la configuración del dispositivo o iniciar una reposición lógica a cero en caso de amenaza de revelación.



Aplicación de PC para el control remoto del R&S®MMC3000.

Interfaz de administración de sistemas de comunicación por bus MIL

El control electrónico de la interfaz de bus MIL del R&S®MMC3000 está albergado en una carcasa separada que puede acoplarse a la unidad base. Es compatible con el estándar MIL-STD-1553B, con acceso redundante incluido. El control remoto se integra en una aplicación de comunicación existente y está orientado a sistemas de comunicación complejos con varios R&S®MMC3000 – principalmente en el ámbito de la aviación, p. ej. helicópteros o aviones.

El módulo de bus MIL del R&S®MMC3000 ofrece plena capacidad operativa, así como cambios de ajustes predefinidos y funcionalidad de reposición lógica a cero.

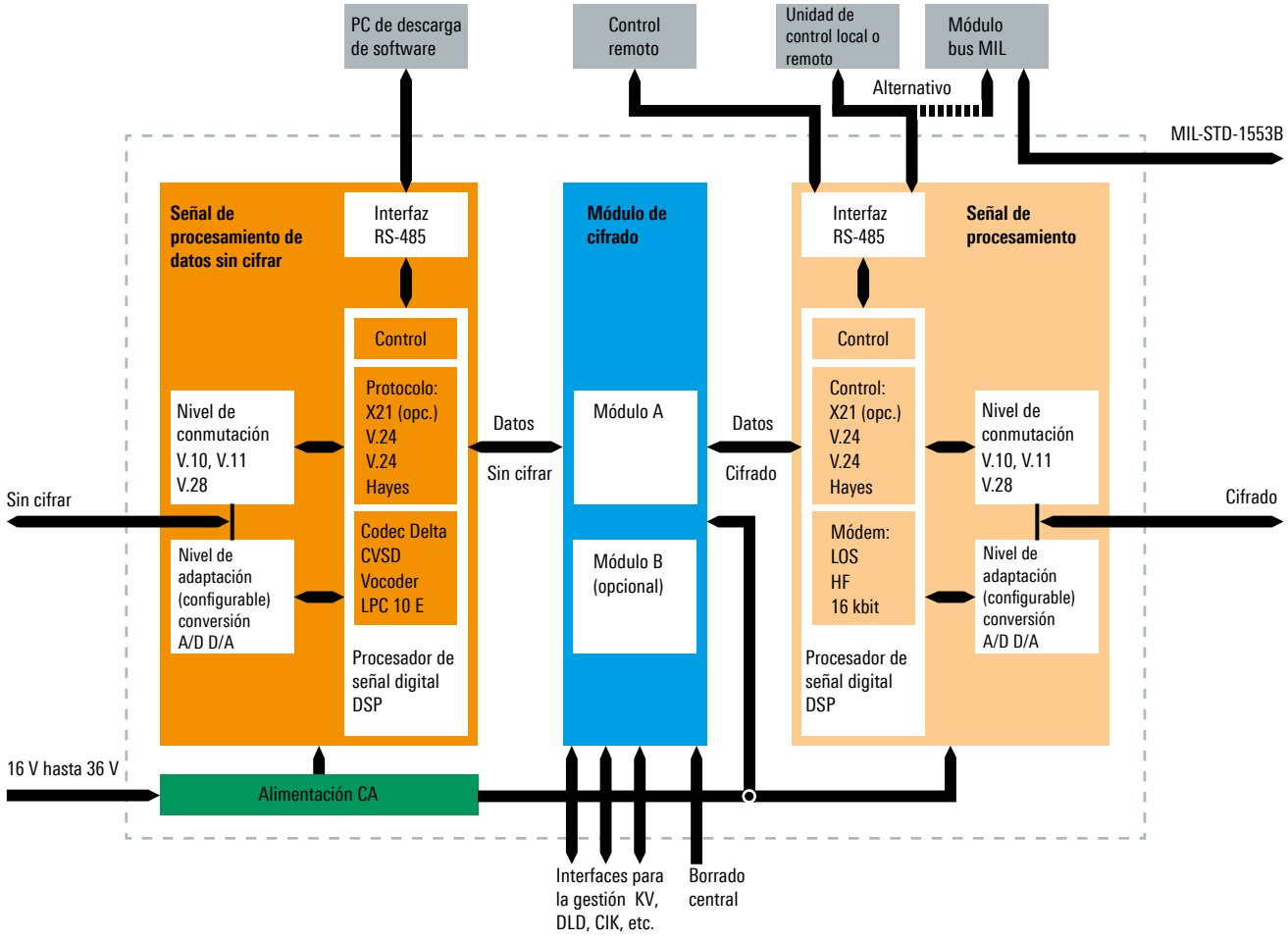
Interfaz del usuario para la unidad de control

La unidad de control del R&S®MMC3000 está albergada en una carcasa separada que se puede acoplar a la unidad base. Está prevista para sistemas de comunicación sencillos con un único R&S®MMC3000, donde un operador local puede cambiar entre los ajustes predefinidos y obtener acceso a todos los ajustes de parámetros lógicos, físicos y de seguridad (p. ej. voltaje, reposición a cero física y lógica, revocación de la reposición a cero). La unidad de control se puede operar además independientemente de la unidad base por medio de un enlace por cable con una longitud de cable de hasta 50 m. Las piezas de conexión para la unidad de control separada están disponibles a pedido.

Interfaz de auriculares/intercomunicación

La interfaz de auriculares/intercomunicación admite tanto micrófonos activos como pasivos y silenciador para una mejor calidad de voz. Se utiliza principalmente para comunicaciones locales de emergencia o para la localización de errores; no requiere una reconfiguración del equipamiento o las aplicaciones conectadas.

Esquema del dispositivo de encriptado R&S®MMC3000



Protección integral gracias a un sofisticado concepto de seguridad

El R&S®MMC3000 está basado en un concepto de seguridad que abarca todo el ciclo de vida de cifrado para una protección integral.

Entorno de producción auditado

El concepto de seguridad del R&S®MMC3000 parte de la misma producción, puesto que se fabrica íntegramente en un entorno de alta seguridad en las fábricas auditadas de Rohde&Schwarz en Alemania.

Separación de hardware rojo-negro y protección contra manipulaciones

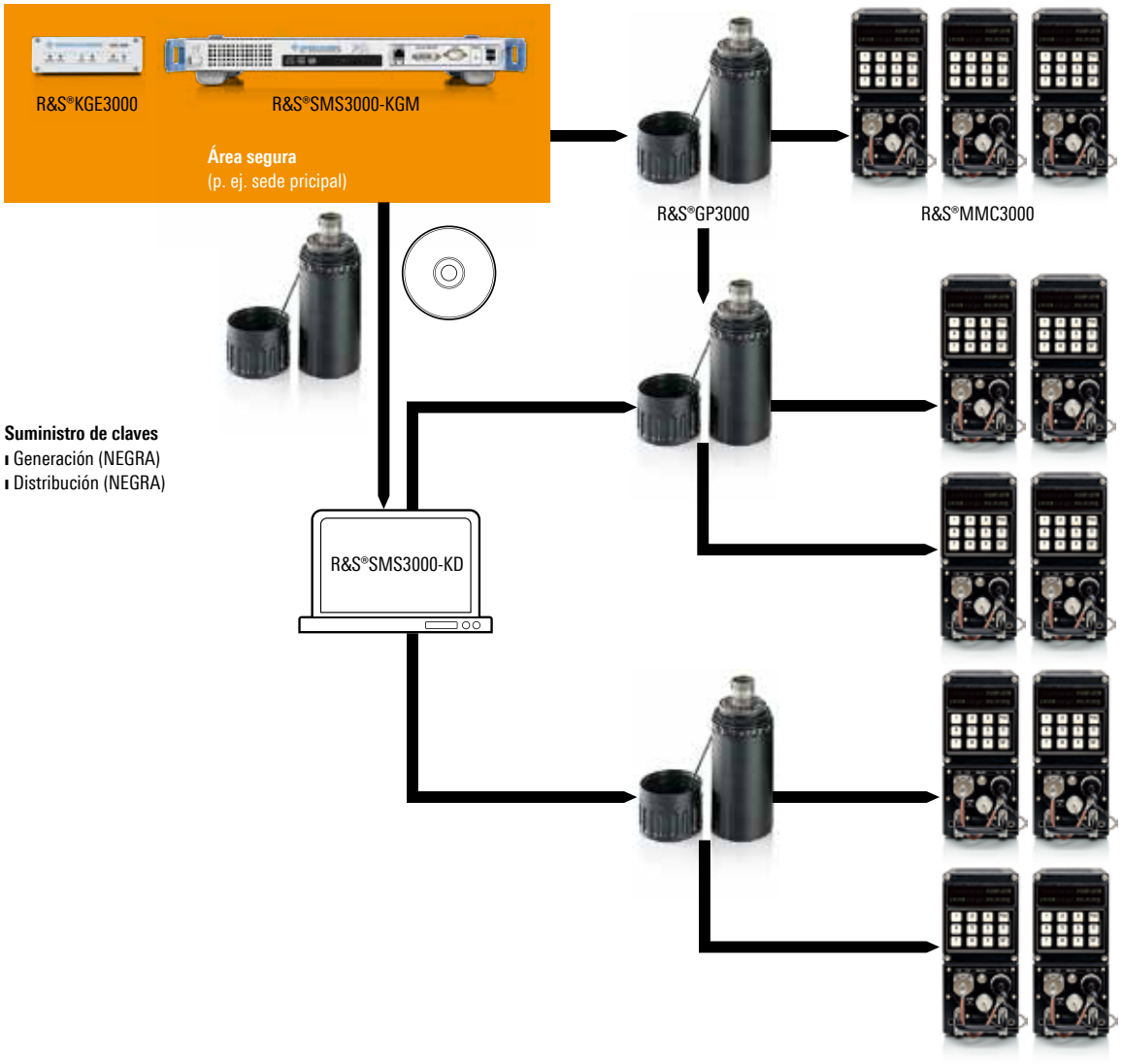
Su separación de hardware rojo-negro garantiza la seguridad de la información a nivel físico. La integridad del R&S®MMC3000 durante la operación está garantizada mediante sofisticados mecanismos de protección contra manipulaciones frente a accesos no autorizados. En caso de emergencia, el dispositivo se puede reponer a cero de forma automática o manual en cada una de las interfaces físicas disponibles. La rutina de prueba incorporada (built-in test, BITE) supervisa constantemente la operación del dispositivo, asegurando el correcto comportamiento del sistema. El diseño con certificación TEMPEST elimina el riesgo de interceptaciones.

Generación y gestión segura de claves

El R&S®MMC3000 ofrece una avanzada gestión variable de cifrado negro así como un sistema de gestión de seguridad de alto rendimiento. Las claves negras que aporta el sistema de gestión de seguridad del R&S®SMS3000 se cargan de forma segura desde el dispositivo de carga de datos (DLD) reforzado R&S®GP3000 al R&S®MMC3000. El proceso de generación de claves se ejecuta en el equipo dedicado a la generación de claves R&S®KGE3000, que incluye un generador de ruido aleatorio físico verdadero (TRNG) de alta calidad.

Si no se dispone de una infraestructura de claves, el R&S®MMC3000 puede generar claves de operación en el dispositivo de cifrado.

Generación y gestión de claves con el R&S®MMC3000



Versatilidad con múltiples modos de tráfico/operación y métodos de transmisión

El concepto flexible de interfaces del R&S®MMC3000, con interfaces de comunicación analógicas y digitales, soporta numerosos modos de tráfico y de operación así como métodos de transmisión.

Modos de tráfico adaptados a los modos de operación y métodos de transmisión

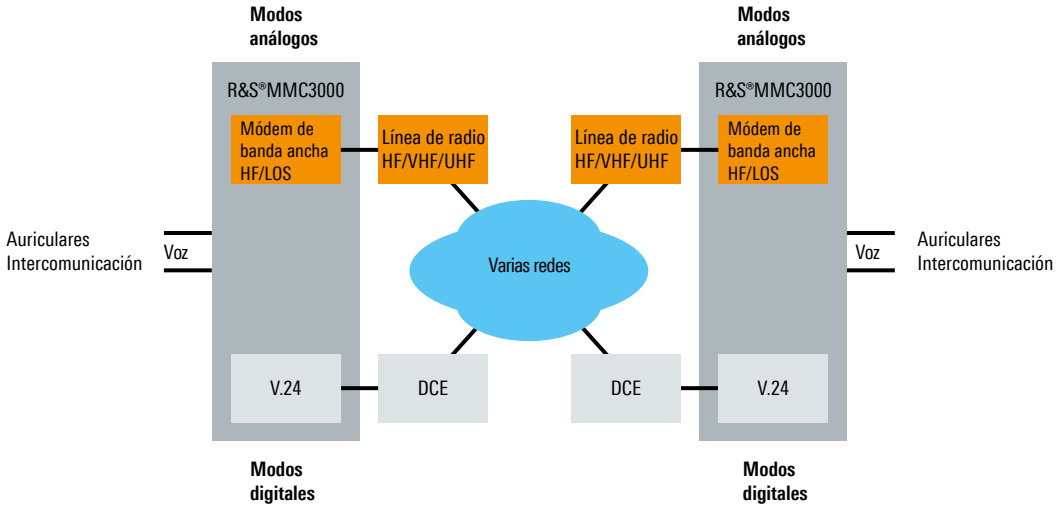
El modo que utiliza el R&S®MMC3000 para enviar voz y datos depende del modo de operación y el método de transmisión seleccionados. Son posibles los modos de tráfico simplex, semi-dúplex (HDX), dúplex, simplex doble (DX), late entry (DX-LE) y dúplex con confirmación (DXD).

Modos de operación para transmisiones de voz y de datos

El R&S®MMC3000 incluye cuatro modos de operación que vienen determinados por el cableado de las interfaces externas y la parametrización. Los modos de operación individuales se parametrizan a través de la unidad de control. Los parámetros ajustados se guardan en la unidad base del R&S®MMC3000. Los modos de operación parametrizados son:

- Cifrado de datos: en el modo de cifrado de datos, el R&S®MMC3000 se puede integrar en sistemas de transmisión de datos provistos de interfaces compatibles con ITU-T V.24/V.10/V.11/V.28 o X.21/V.11 (opcional). Se pueden utilizar protocolos de marcado o comandos Hayes (comandos AT); una vez que los comandos Hayes enviados a través del equipo terminal de datos (STE) han sido identificados y verificados, el R&S®MMC3000 reenvía los comandos Hayes, sincroniza la estación llamada y activa el modo de datos encriptados. Si se utiliza una interfaz analógica, se emplea el módem LOS integrado (conforme a ITU-T V.26) o el módem HF (conforme a STANAG 4197)
- Cifrado de voz: en el modo de cifrado de voz, las señales de voz son digitalizadas bien por el codificador de voz LPC 10e o bien por el códec delta CVSD, según el modo de tráfico. Se puede seleccionar un módem HF (conforme a STANAG 4197), un módem LOS (según ITU-T V.26), modo banda base/bifase o V.24, dependiendo del método de digitalización de voz seleccionado
- Voz sin cifrar/datos sin cifrar: están disponibles varios modos sin cifrar para voz y datos en función de las distintas aplicaciones (voz: modos HF, VHF, UHF; datos: modo V.24 digital)

Cifrado de voz en diferentes redes de comunicación



Teletipo para una fiabilidad extrema en las comunicaciones

El teletipo hace posibles comunicaciones extremadamente fiables en entornos con ancho de banda reducido y variable, pero requiere una adaptación flexible a niveles de voltaje bajos.

- Las velocidades de transmisión desde 50 bit/s hasta 64 kbit/s permiten cursar comunicaciones en numerosos escenarios extremos y especializados, p. ej. velocidades de transmisión reducidas en comunicaciones para helicópteros o transmisiones VHF/UHF
- La interfaz de auriculares admite tanto micrófonos activos como pasivos y silenciador para una mejor calidad de voz. Es posible configurar la integración de canal de protección. Igualmente, a través de la interfaz se puede realizar la comunicación de emergencia local y/o la localización de errores sin necesidad de configurar el equipamiento/las aplicaciones conectadas

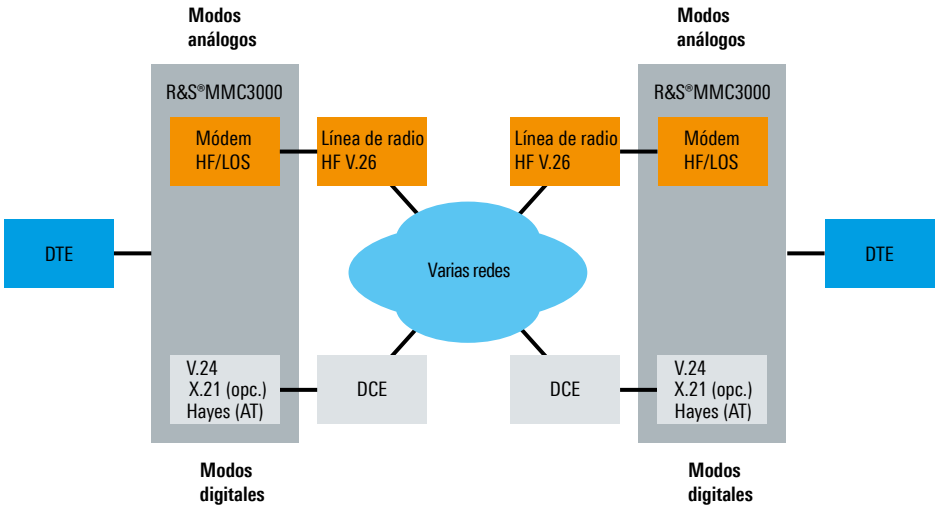
Preparado para transmisiones vía IP

La transición al tráfico IP para la información de carga útil está contemplada en las infraestructuras Ethernet. Los datos se conducen tunelizados a través de Ethernet mediante convertidores estándar, lo que elimina las limitaciones de las transmisiones en serie en materia de distancia.

Transmisiones síncronas y asíncronas a través de las interfaces roja y negra

Todas las combinaciones de transmisiones síncronas y asíncronas están contempladas tanto en la interfaz de cifrado negro como en la interfaz de cifrado rojo. Los diferentes requisitos de temporización entre redes separadas se satisfacen sin necesidad de incorporar equipamiento adicional o modificaciones en la red.

Cifrado de datos en diferentes redes de comunicación



Alta calidad de servicio y operación flexible con tecnología de vanguardia

Alta calidad de servicio

El R&S®MMC3000 responde a la demanda de máxima calidad de servicio bajo diferentes condiciones:

- "Late entry" garantiza una comunicación cifrada ininterrumpida incluso bajo condiciones difíciles del canal de transporte
- Códecs de voz de alta calidad optimizados para cada tipo de transmisión

Configuración flexible

Cinco páginas de ajustes predefinidos para cada modo de operación facilitan la configuración rápida y flexible.

Posibilidad de actualización

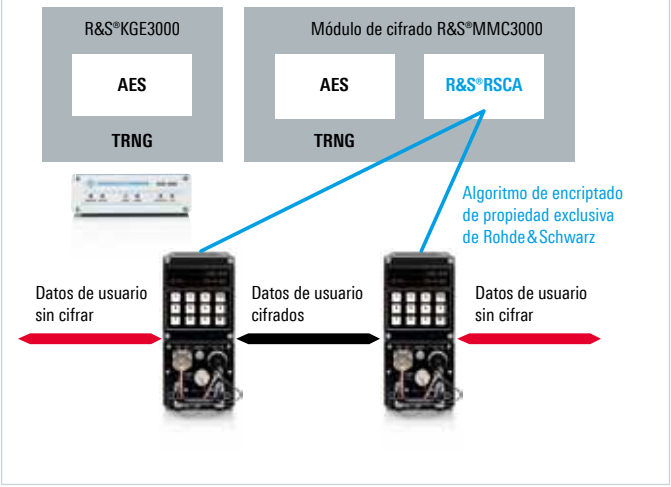
El R&S®MMC3000 incluye una ranura adicional para la integración futura de un módulo de cifrado.

El R&S®MMC3000 se puede actualizar a través de una descarga de software protegida utilizando un PC y un paquete dedicado a la descarga de software. Este mecanismo está protegido por el algoritmo de cifrado específico del cliente.

Configuración individual mediante algoritmos de cifrado personalizables para requerimientos específicos del usuario

El encriptado del R&S®MMC3000 se basa en el módulo de cifrado SIT de alto rendimiento de Rohde&Schwarz. La adaptación a las exigencias del cliente es posible a través del algoritmo de propiedad exclusiva R&S®RSCA y/o la implementación específica del algoritmo AES 256. El alcance de la personalización se puede adaptar para satisfacer de forma precisa y exclusiva los requerimientos de distintos clientes y aplicaciones. Rohde&Schwarz SIT controla todos los aspectos del ciclo de vida del cifrado, y por lo tanto los elementos adicionales, como contenedores de cifrado, material de generación de claves, claves para el cifrado de claves y cargadores de claves, están configurados de tal modo que garantizan la integración perfecta de los algoritmos implementados.

Tecnologías de seguridad del R&S®MMC3000



Operación y puesta en servicio simplificada con una amplia gama de accesorios

Un PC de configuración aumenta la eficiencia y precisión del proceso de carga de ajustes predefinidos

La aplicación para la (pre)configuración de ajustes predefinidos y la carga de los mismos en una serie de R&S®MMC3000 evita errores por parte del operador durante la puesta en servicio del sistema.

La clave de ignición de cifrado (crypto ignition key, CIK) añade un nivel de seguridad adicional e incrementa la flexibilidad en la implementación

Con esta opción, el R&S®MMC3000 solo está operativo cuando se ha introducido la CIK en el dispositivo. La CIK protege el acceso a la memoria variable de cifrado y, una vez que se retira, el R&S®MMC3000 puede dejarse sin vigilancia sin peligro de que pueda extraerse la información secreta del dispositivo. Esto no solo amplía la variedad de escenarios posibles de aplicación, sino que además permite reaccionar rápidamente en casos de riesgo inmediato.

El armazón de montaje protege al dispositivo en entornos con condiciones físicas severas

Un armazón de montaje conforme con los estándares militares garantiza la instalación segura del R&S®MMC3000 en entornos especialmente expuestos a golpes, choques y fuertes vibraciones, como p. ej. en helicópteros.

El dispositivo de carga de datos R&S®GP3000 (DLD) facilita la distribución de claves a unidades distribuidas geográficamente

Con el DLD ya no es necesario reunir todas las unidades en una misma ubicación cercana al equipo o al proceso de generación de claves. Gracias a la carga de claves negras en el R&S®MMC3000, el proceso de carga de claves es totalmente seguro, incluso en caso de pérdida de un DLD.

Fuente de alimentación externa de adaptación continua (110 V/240 V)

El voltaje de la fuente de alimentación abarca de 16 V a 36 V. La fuente de alimentación tiene protección EC y ofrece opciones de interfaces para diferentes conectores.

Componentes y equipamiento para el R&S®MMC3000

Especificaciones

Especificaciones		
Datos de operación		
Modos de operación		voz SIN CIFRAR/ENCRIPTADA, datos SIN CIFRAR/ENCRIPTADOS
Modos de tráfico		semidúplex (voz) simplex semidúplex (HDX) simplex doble (DX) dúplex con confirmación (DXD) late entry (DX-LE)
Interfaz analógica		
Audio		
Interfaz de audio/intercomunicación universal de cuatro hilos		
Nivel		–47 dB hasta +13 dB, ajustable en etapas de 1 dB
Impedancia		600 Ω
Auriculares		interfaz para auriculares
Radio		banda estrecha/banda ancha
Nivel		–40 dB hasta +20 dB, ajustable en etapas de 1 dB
Impedancia		600 Ω
Modo de tráfico		semidúplex
Método de transmisión		BANDA BASE/BIFASE módem LOS (V.26) módem HF (STANAG 4197)
Procesamiento de voz		códec delta (CVSD) 16 kbit/s LPC 10E (2.4 kbit/s) conforme a STANAG 4198
Interfaz digital		
V.24		asíncrono 50 bit/s hasta 57.6 kbit/s (5/7/8 bits) asínc./sínc. 50 bit/s hasta 19.2 kbit/s (5/7/8 bits) síncrono 50 bit/s hasta 64 kbit/s apto para comandos Hayes
Otras interfaces		
Entrada de claves		RS-485 (DLD)
Borrado de emergencia de claves (reposición a cero)		conmutador borrado central
Bus MIL		MIL-STD-1553B
CIK		clave de ignición de cifrado
Control remoto mediante aplicación de PC	para hasta 31 R&S®MMC3000	RS-485
Datos de operación y almacenamiento		
Temperatura de operación		–30 °C hasta +70 °C
Temperatura de almacenamiento		–40 °C hasta +85 °C
Fuga RF		Probado
Compatibilidad electromagnética		MIL-STD-461C categoría A1b, parte 2
Datos generales		
Dimensiones	alto × ancho × prof.	193.5 mm × 90.4 mm × 200 mm
Peso		3.8 kg
Corriente de alimentación		28 V (16 V hasta 36 V) CC
Alimentación	entrada	100 V hasta 240 V CA, 50 Hz hasta 60 Hz
	salida	24 V CC
Consumo		< 15 VA
MTBF (tiempo medio entre fallos)		> 8000 h

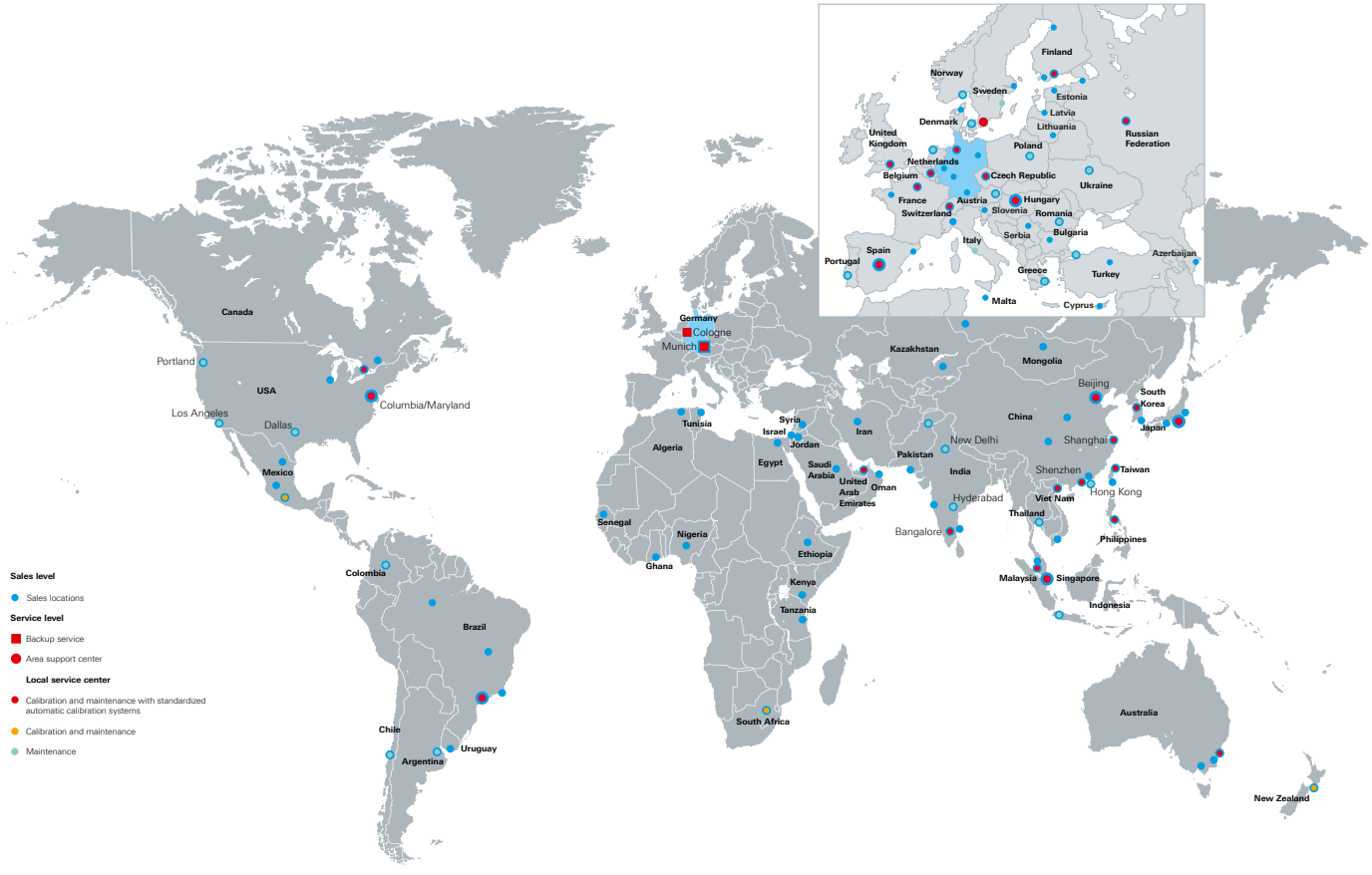
Información para pedidos

Denominación	Tipo	Nro. de referencia
Unidad base (incluye unidad base, unidad de control, armazón de montaje, manual de usuario compacto)		
Dispositivo de encriptado multirrol multimodo R&S®MMC3000	R&S®MMC3000	3566.2805.02
Manual R&S®MMC3000	R&S®MMC3000	3566.1344.32
Manual del integrador R&S®MMC3000	R&S®MMC3000	3566.2811.32
Manual de control remoto R&S®MMC3000	R&S®MMC3000	5401.1635.32
Accesorios		
Módulo de bus MIL	R&S®MMC3000	3545.0603.03
Unidad de control	R&S®MMC3000	3545.0003.03
Armazón de montaje	R&S®MMC3000	3544.5330.04
Fuente de alimentación CA	R&S®MMC3000	3566.0290.00
Unidad de control separada	R&S®MMC3000	3566.2811.02
Software de control remoto	R&S®MMC3000-RC	5401.1635.00
Fillgun (incl. cable adaptador)	R&S®GP3000	3566.2792.02
Estación de gestión de claves (incl. R&S®KGE3000)	R&S®SMS3000-KGM	3566.2705.02

Desde el asesoramiento inicial hasta el servicio postventa: siempre cerca del cliente.

Rohde&Schwarz está presente en más de 70 países, donde cuenta con excelentes profesionales que aseguran una óptima asistencia in situ. Nuestros clientes pueden confiar a nuestros expertos todas las fases del proyecto con el mínimo riesgo:

- Determinación de la solución/adquisición
- Implementación técnica/desarrollo de aplicaciones/ integración
- Capacitación
- Operación/calibrado/reparación



Servicio fiable
- En todo el mundo
- Local y personalizado
- Adaptado al cliente y flexible
- Calidad que no transige
- Confiabilidad de largo plazo

Sobre Rohde&Schwarz

Rohde&Schwarz es un grupo independiente de compañías especializadas en electrónica. Somos proveedor líder de soluciones en los campos de prueba y medición, radiodifusión, radiomonitoreo y radiolocalización, así como comunicaciones seguras. Establecida hace más de 75 años, Rohde&Schwarz tiene presencia global y una red de servicios dedicada en más de 70 países. La sede central de la compañía se encuentra en Munich, Alemania.

Compromiso con el medio ambiente
- Productos energéticamente eficientes
- Mejora ecológica continua en mantenimiento ambiental
- Sistema de gestión del medioambiente certificado según ISO 14001

Certified Quality System
ISO 9001

Rohde&Schwarz SIT GmbH
Am Studio 3 | D-12489 Berlin
Teléfono +49 30 65884-223 | Fax +49 30 65884-184
Correo electrónico: info.sit@rohde-schwarz.com
www.sit.rohde-schwarz.com

www.rohde-schwarz.com

Contacto regional
- Europa, África, Medio Oriente
  +49 89 4129 123 45
  customersupport@rohde-schwarz.com
- Norteamérica
  1 888 TEST RSA (1 888 837 87 72)
  customer.support@rsa.rohde-schwarz.com
- Latinoamérica
  +1 410 910 79 88
  customersupport.la@rohde-schwarz.com
- Asia/Pacífico
  +65 65 13 04 88
  customersupport.asia@rohde-schwarz.com

R&S® es una marca registrada de Rohde&Schwarz GmbH&Co. KG.
Nombres comerciales son marcas registradas de los propietarios
Impreso en Alemania (ch) | PD 0758.2548.17 | Versión 03.00 | Septiembre 2011
R&S®MMC3000 | Datos sin límites de tolerancia no son obligatorios
Sujeto a cambios
© 2003 - 2011 Rohde&Schwarz GmbH&Co. KG | 81671 München, Alemania